California Franchise Tax Board (FTB)

Enterprise Architecture Definition
Identity and Access Management (IAM)

Version No. 1.1

April 11, 2008

Author:
Enterprise Architecture Council

Document Information

Document Source

This document is controlled through Document and Deliverable Management. To verify that this document is the latest version, contact Enterprise Architecture.

Revision History

Version No.	Date	Summary of Changes	Revision Marks
1.1	2/05/2008	Formatting changes	John R.

Table of Contents

List of Figures

1.0 Executive Summary and Charter

1.1 Overview

Identity and Access Management (IAM) will provide FTB security as a business service, and a method to ensure all individuals and services are properly authenticated, authorized and audited when accessing application services. The IAM solution will provide a centralized and consistent security policy and will be delivered in a “security as a service” strategy, removing the responsibility of writing security code from FTB developers. To be effective, the security service will be integrated with an Enterprise Service Bus (ESB) allowing these services to be discoverable and usable for all web services throughout the department regardless of the system or business unit.

1.2 Scope

Identity management and access control for FTB’s external and internal users in an SOA environment provides an integrated standards-based solution that delivers authentication, web single sign-on, access policy creation and enforcement, user self-service, delegated administration, reporting and auditing.

1.3 High-level Requirements

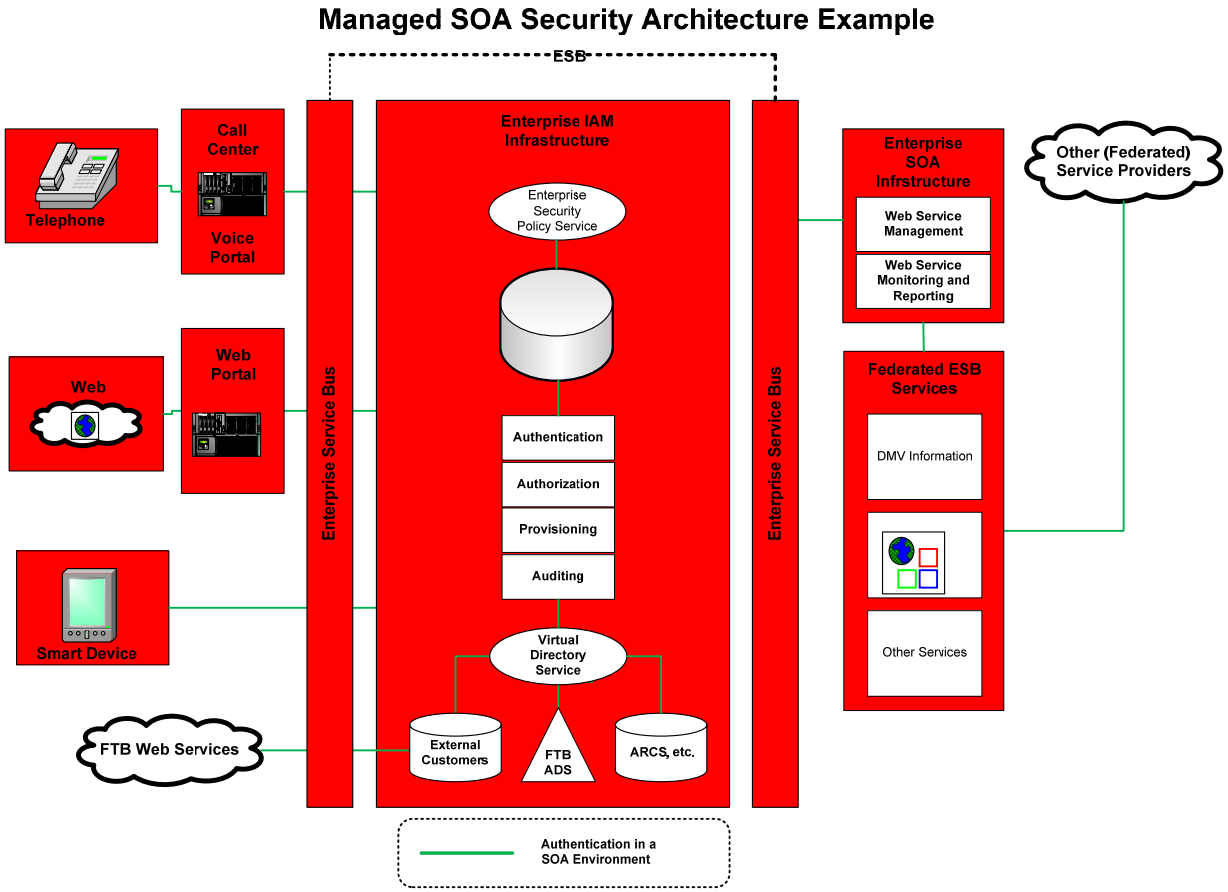
Figure 1.3-1: High level requirements

Requirement	Description
Provide Centralized Authentication for the Enterprise	Leverages existing authentication mechanisms to make it easier to integrate with existing environments
Provide Distributed Authentication	Secures applications with minimal security risk and maximum deployment flexibility
Single Sign On capability	Ensures that existing sign-on mechanisms can be leveraged across Web applications, federated partners, and Web Services
Real Time Management	Provides a centralized view of who is accessing resources
Provide a centralized policy that defines access control policies	Ensures only authorized users access protected resources
Flexible Data Store Support	Allow administrators to separate policy and configuration information from user data. Prevents duplication of user data by using a centralized security solution on existing directory services.
Open Standards Based	Uses standards such as SAML and ID-FF to create and share security for federation and easy upgrade and redeployment.
Access Auditing and Event Logging	Provides a trail of access for auditing violations.
Easily Scalable	Scales to meet the growing requirements of enterprises and service providers

1.4 Conceptual Architecture Model

The AIM architecture will be an integrated IAM solution within an SOA environment providing security as a service. The SOA infrastructure will be capable of supporting composite applications comprised of underlying reusable services that do not contain hard-coded security controls. Access to internal applications will be secured by the IAM solution.

Figure 1.4-1: Managed SOA Security Architecture Example



2.0 Current Capabilities and Components

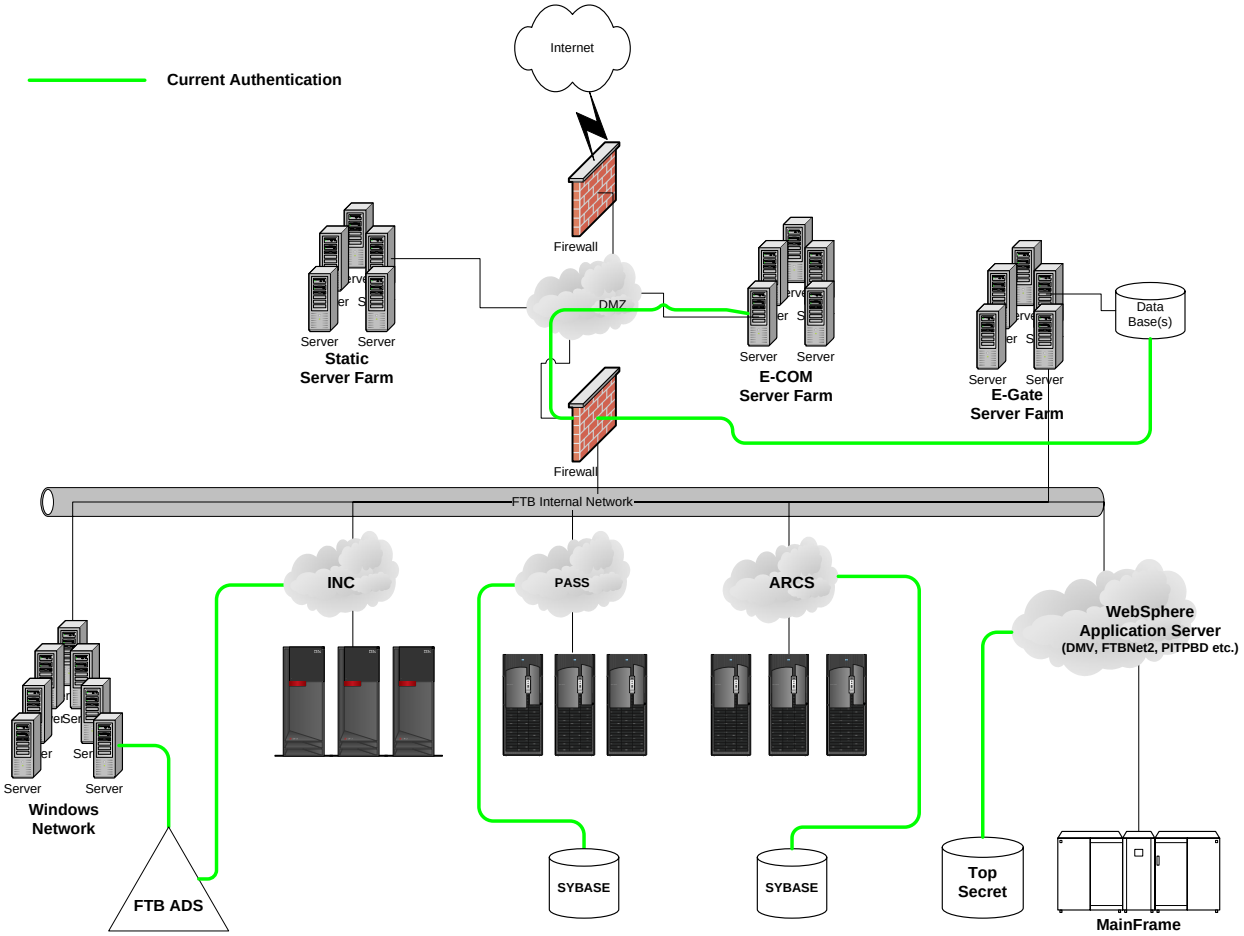
2.1.1 FTB current security

FTB has developed applications as stovepipe solutions. Each application developed its own authentication, authorization, auditing and user provisioning code and procedures. The main tax processing applications have either relied on the Top Secret security service (legacy applications) or developed individual data base systems for security (PASS, ARCS etc.). The result was the development of separate security groups who control access to the various systems throughout the department and the development of specialized security code using various methods for system auditing. This also complicates de-provisioning when employee's duties change or they leave FTB employment.

IAM governance is a combination of identity auditing, role-management and enforcement of security policies as they apply to the enterprise. FTB has change management, an IT service desk and is developing a problem resolution section following the ITIL principles.

Enterprise Security is managed by platform type using a variety of methods. Over the past several years, the majority of new and updated applications have been designed to leverage Microsoft Active-Directory (AD). Application developers create security routines that validate identity and role access via AD API calls. FTB does not have an integrated IAM system that governs access to the various tax systems. Authentication is performed by comparing credentials against information stored inside a system peculiar database (ARCS), Microsoft's Active Directory (AD), SQL database or for mainframe based applications – CA's Top Secret security server. In recent years, many of FTB's internally developed applications have been written to leverage the AD API interfaces for security, or hosted on WebSphere, which uses Top Secret to perform authentication.

Figure 1.4-1: "As-Is" Technical Architecture



3.0 Target Architecture

3.1 Future Capabilities and Components

Identity management simplifies the process of managing user identities across a variety of applications in order to provide provisioning and secure access, ensure ongoing compliance and enable federation for sharing beyond boundaries.

Identity management involves administration and policy creation, while access management entails enforcement of those policies. Together, IAM is a hierarchical collection of security practices and technologies, each new stage building on the prior one.

FTB will provide capabilities to enterprise applications and services to simplify user experience by reducing the number of times users log into protected resources. We will establish federated security with other state agencies through seamless access using open standard based protocols. The Data store will deliver information and services to users efficiently and cost-effectively no matter how business needs change or user requirements grow. The service delivers a set of capabilities to provide a centralized data store for users' identity data and for supporting data that can be leveraged for Web services architectures. Finally, the IAM infrastructure will support an SOA environment.

3.1.1 Identity and Access Management

IAM will provide complete capabilities to both detect and prevent compliance violations. An enterprise solution will make it possible to detect and remediate existing policy violations using automated processes. Without an enterprise solution, detecting policy violations can take weeks. Identity management provisioning and identity auditing capabilities is key to helping FTB achieve regulatory compliance at a reasonable cost as FTB moves to adopt National Institute of Standards & Technology (NIST).

IAM will simplify how users gain access to applications, provide SSO capabilities to Web applications, portals, windows desktop environments, applications, and loosely coupled Web services using a centralized set of authentication mechanisms and secure-access policies.

The IAM systems will intercept requests to applications or services and determine whether the user has been properly authenticated. Once authenticated, the user's credentials are verified using a central user profile repository (Metadirectory) and policy store that determines whether the user will be permitted to access the resource. If the user has not previously been authenticated, they are prompted with a login challenge to supply a username and password or other type of credential.

Administrators will have a clear view of which users are signed onto which resources, thus providing centralized control over application security.

3.1.1.1 External Authentication for Secure E-Services

FTB plans to leverage its implementation of its reverse proxy with our current secure web architecture to implement an enterprise authentication solution to provide an Identity and

Access Management solution. Solutions for this project will support the following standards for web services security:

- Web Service Security (OASIS standards)
- Web service authentication and authorization
  - SAML, XACML
- W3C XML encryption standard
- XML Signature (Wc3) and X.509 certificates
- Security for UDDI (OASIS standard)

*3.1.1.2 **Web SSO***

As FTB moves to provide customers a single web portal to access applications, Web SSO will be needed to enable users to sign on once and get access to all services, which they're authorized to use.

*3.1.1.3 **Self Serve Registration***

As FTB moves to implement an opt-in method of providing access to web based applications, implementation of a self-registration service will be needed to give users access by proving who they said they are.

*3.1.1.4 **Federation***

Integrated federation services will allow FTB to extend core authentication and authorization services with partners via standards based security. These standards include the Security Assertion Markup Language (SAML) and Liberty Identity Federation Framework (ID-FF). FTB's federation will allow users to link accounts across partner sites and generates a security assertion for each user, creating a seamless, simple sign-on experience.

*3.1.1.5 **Data Services***

Horizontal in nature, the data service will be the core component of the IAM solution, providing a central repository that contains profile information, passwords, through data supports, such as, flat files, databases, directories, etc. This service will be compliant with the Lightweight Directory Access Protocol (LDAP). Until it is feasible to consolidate to one data store, FTB will use more than one directory. Therefore, it is important to have only one entry for all existing directories to facilitate and centralize management. This metadirectory will create a global view of isolated identity information stored in multiple locations.

*3.1.1.6 **Provisioning Service***

This will allow centralized and automated management of user accounts and entitlements across multiple applications and directories. This will be related to FTB's operational procedures for account creation modification, retirement and deletion. Provisioning will verify identity to fulfill approval. Provisioning has the capabilities to manage identities across disparate systems.

3.1.2 Reverse Proxy

A reverse Proxy Server will provide access to ecommerce web applications while providing network isolation from external customers, and prevents the disclosure of internal network addresses and network addressing schemes. Reverse proxy servers will simplify firewall rule sets by reducing the number of trusted IP addresses that are allowed to access internal resources. This service will automatically route requests on behalf of the user appropriately

through a referral mechanism and provides secure firewall-like services. The requester's original packets are interpreted and never sent to the backend systems.

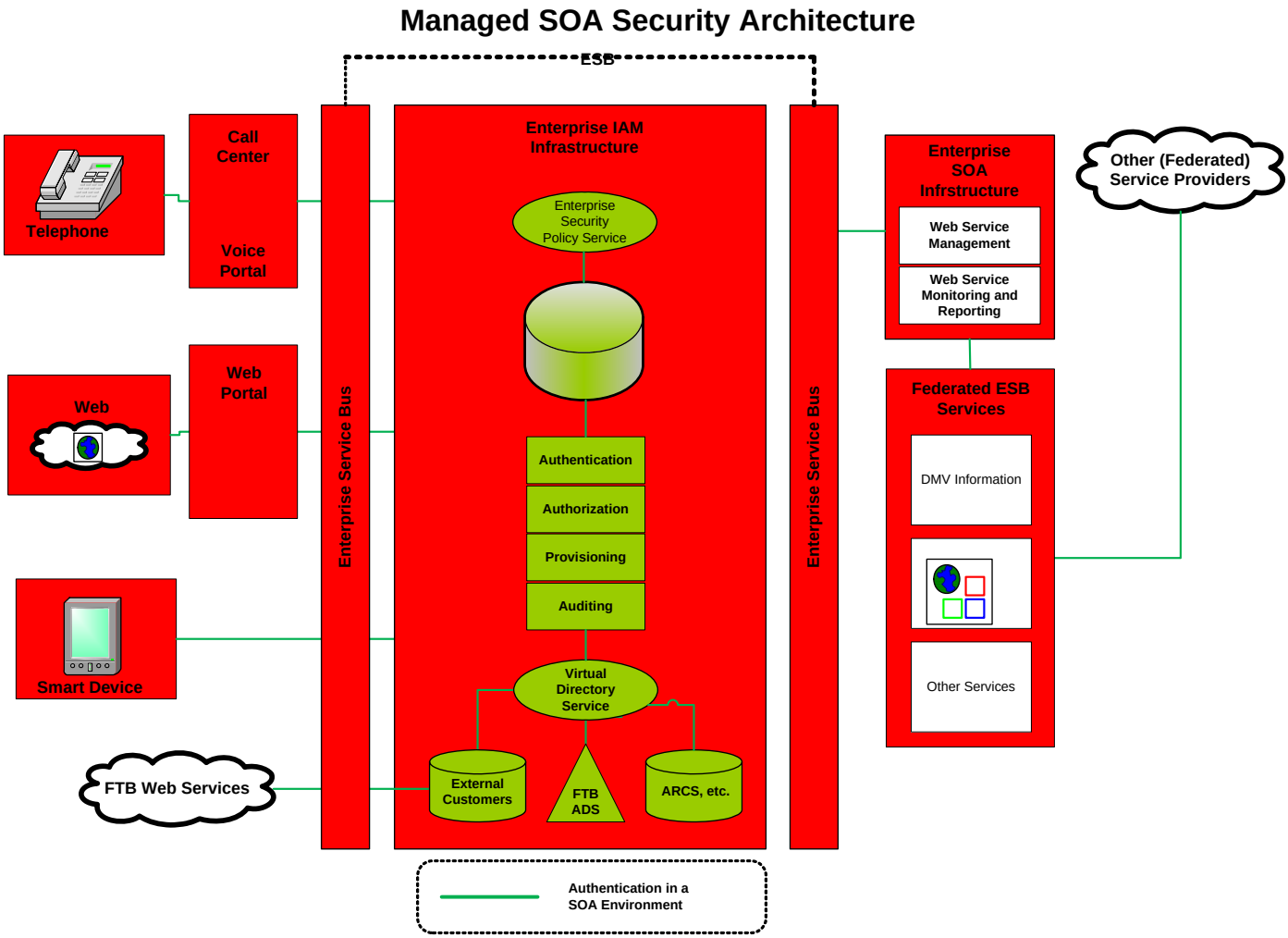
3.1.3 SOA environment

SOA environment will comprise of several components:

- An Enterprise Service Bus
- A Service Registry (UDDI)
- A Governance Module for web service security enforcement
- A management interface to control the web service environment.
- Voice and web portals
- Various databases to store service and policy information

The SOA infrastructure can be thought of as a composite application that is made up of underlying reusable services that should contain no hard-coded security controls. In order to ensure that this "application" is secure, it will need an IAM solution, which is a set of real-time security services externalized from and consumable by all the underlying applications (services), configured via policy and enforced for compliance. The IAM must be an integral part of the SOA infrastructure, so that as new or changed business services are designed, developed and deployed, accesses to them are controlled and audited. This design will allow the business or policy needs to change, while the security services infrastructure will dynamically adapt.

Figure 3.1-1: Managed SOA Security Architecture



*3.1.3.1 **Web Portal***

The Web Portal functions as a central point of access to information. This will provide FTB with a consistent look and feel with access control and procedures for multiple applications (services). In a SOA environment, these services may exist on another trusted network without the user needing to be aware of its location.

3.1.4 Enterprise SOA Infrastructure

This includes Web Services Management that is used to provide visibility and control required to deploy Web Services into production and allows control and administration of a common security infrastructure for all Web Service applications. This allows for implementing best practice security policies and Web Service monitoring for all managed services. This works by:

- Decrypting XML messages
- Authenticating user credentials

- Perform authorization checks for users and Web Services
- Create and manage audit logging
- Submitting security messages to the intended Web Service

3.1.5 Enterprise IAM Governance

FTB will create a governance body that will oversee, control and regulate the IAM process. It will follow three major phases:

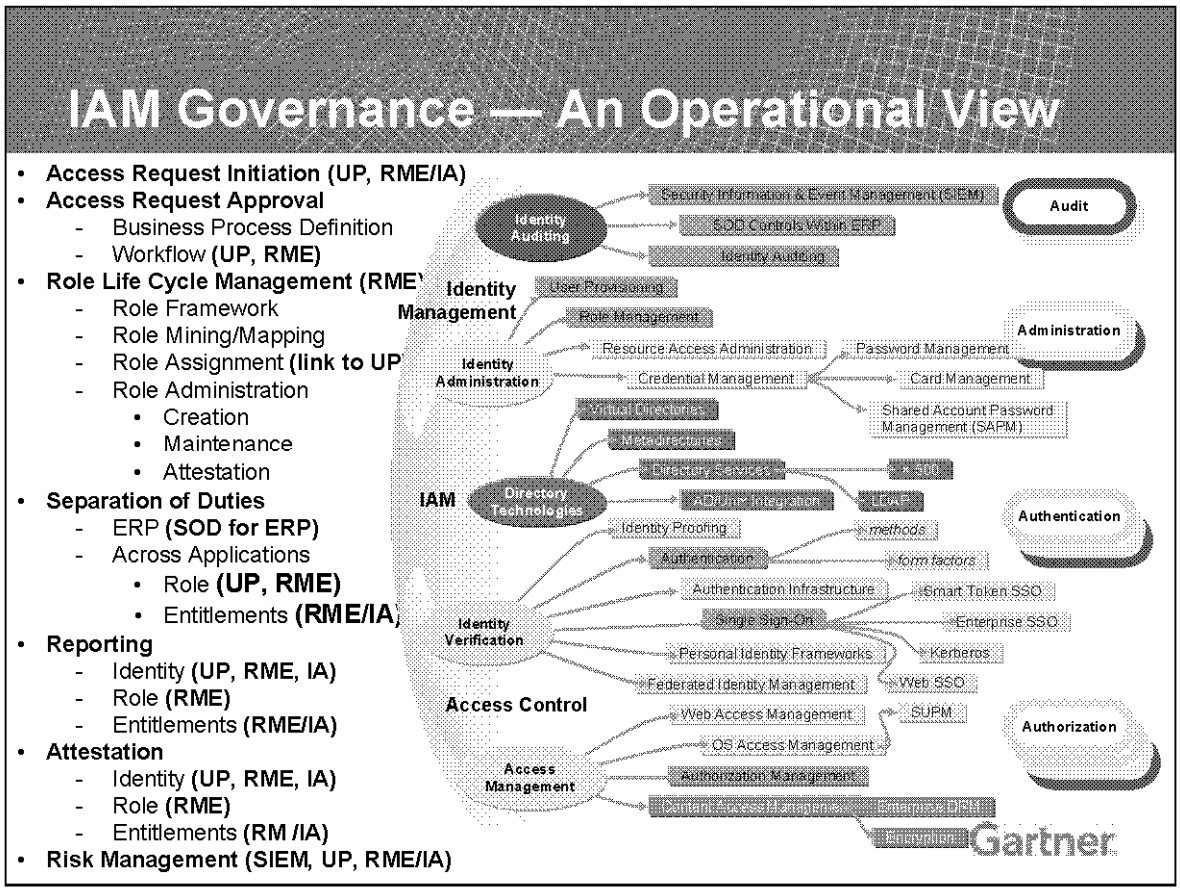
1. Establish control objective – this needs to be done to minimize the risk to the enterprise. An example of this developing clear guidelines for application development and/or infrastructure deployment
2. Implement controls – these are the processes and procedures that are required to meet the control objectives.
3. Establish a centralized auditing program – this provides proof that the controls are actually in place and are working.

An overall look at the operational view of IAM Governance lists activities that the enterprise needs to address for user identities, roles and, most importantly, authorization entitlements:

- Access request initiation — by the end user, manager, security administrator, or HR representative
- Access request approval, including the definition of the business approval flow, that is, who can approve an access request, when the request needs to be escalated, and so forth
- Role life cycle management, including the establishment of the role framework, role mining/mapping, role assignment (this would include a link to a user provisioning product), and role administration, including creating, maintaining and attesting to the role
- Reporting of identity information for identities, roles and authorization entitlements
- Attestation of identity information for identities, roles and authorization entitlements
- Access risk management — reviewing not only what a user has been granted access to, but what they are using so that their role assignments are appropriate (From Gartner 11/07 IAM Summit)

The following figure is a breakdown of IAM Governance activities and associated processes that should be in place:

Figure 3.1-2: Operational View of IAM Governance



4.0 Gap Analysis

Figure 3.1-1: Gap Analysis

GAP	Success Factor	Benefit
Identity data is duplicated across the enterprise in different data stores	Centralized , automated identity management	Reduced complexity and reduces cost
Disparate platforms	Virtual centralization of data store. Centralization of security policy	No redundant data. Can have a central IAM with multiple platforms
Disparate authentication access controls	Role based authentication with reusable access control policies	Centralized, automated identity management
Security Policies are inconsistent	Centralized automated security policies.	Consistent control of security policies
Diverse user base with differing level and types of access	Role based authentication with reusable access control policies	Easier to manage and audit
No Enterprise auditing and reporting	Virtual identity profile which has a single view and single point of management	Improved security though knowledge
No enterprise remediation	Automated remediation through all systems with session termination	Improved security through fast and affiant remediation. Automation
No enterprise metric capabilities	Automated compliance reporting reviews for standard compliance such as Sarbanes-Oxley and HIPAA	Able to establish compliance to legislation.
Web self registration	Implementation of web self registration.	Reduced overhead. Improved customer service.

5.0 Roadmap

In order to migrate from our current authentication and access methods, FTB should consider the dependencies that FTB's SOA strategy will have on currently planned projects.
The following is the recommendation on how to phase-in departmental IAM from our current systems, capabilities and workloads. There are main phases outlined below.

Figure 3.1-1: Security and Identity Management Roadmap

ID	Task Name	Scheduled Work	Percent Complete	Duration	Start Date	Finish Date	Predecessors
1	Start phase I of IAM	1,180 hrs	0%	202 days	03/11/2008	12/17/2008	
2	Determine requirements for IAM Phase I	300 hrs	0%	37 days	03/11/2008	04/30/2008	
3	Submit Project for Bid	80 hrs	0%	43 days	05/01/2008	06/30/2008	2
4	Select Vendor	100 hrs	0%	1 day	07/16/2008	07/16/2008	3
5	Implement product	700 hrs	0%	110 days	07/17/2008	12/17/2008	4
6	Start Phase II of IAM	4,000 hrs	0%	412 days	12/18/2008	07/16/2010	5
7	Determine requirements for Phase II of IAM	400 hrs	0%	87 days	12/18/2008	04/17/2009	
8	Submit Phase II Project for Bid	80 hrs	0%	42 days	04/20/2009	06/16/2009	7
9	Select Vendor	100 hrs	0%	1 day	07/15/2009	07/15/2009	8
10	Implement Proposed Phase II IAM solution	3,420 hrs	0%	262 days	07/16/2009	07/16/2010	9

5.1.1 First Phase

The first phase in deployment of an IAM solution would be to enable identity management for external customers accessing web applications. This is a mature technology providing the following benefits:

- Enables customers with a single sign on to the applications that they are entitled to use.
- Provides centralized control for application security.
- Protects applications by providing an enterprise security policy.
- Provides the ability to extend core authentication and authorization services with partners via standards-based security assertions (including SAML and ID-FF) for Federated Identity.

5.1.2 Second Phase

The second phase for IAM deployment would be to provide a comprehensive IAMS solution that will interface with the phase I deployment web SSO solution and will provide the following services:

- User provisioning
- Role based access management
- Access Management
- Auditing services
- Centralized security policy service

6.0 Appendix

6.1.1 Best Practices

To ensure a secure environment for a Service Oriented Architecture (SOA) environment, it is imperative that all types of individuals and entities (including services) are properly identified, authenticated and managed. FTB will deploy a security service that is external to, but accessed by all applications and services, with best practice being to procure rather than develop. Developers will design business logic instead of writing security code inside their applications. The IAM solutions chosen as a governance system for an SOA environment will be capable of interfacing with Federated IAM systems and be compliant with the California Enterprise Architecture Program (CEAP) vision for statewide (Federated) identity management.

Federated Identity Management is now at a maturity level where it is ready for practical use, as it should be a mainstream technology within 2 to 5 years. Other security technologies that currently considered mature and ready to deploy include Enterprise Single Sign On (ESSO), Web Access Management (WAM) and strong authentication systems (two factors) which support smart card or token technologies. FTB will use the industry common open standard, Security Assertion Markup Language (SAML).

6.1.2 Industry Trends

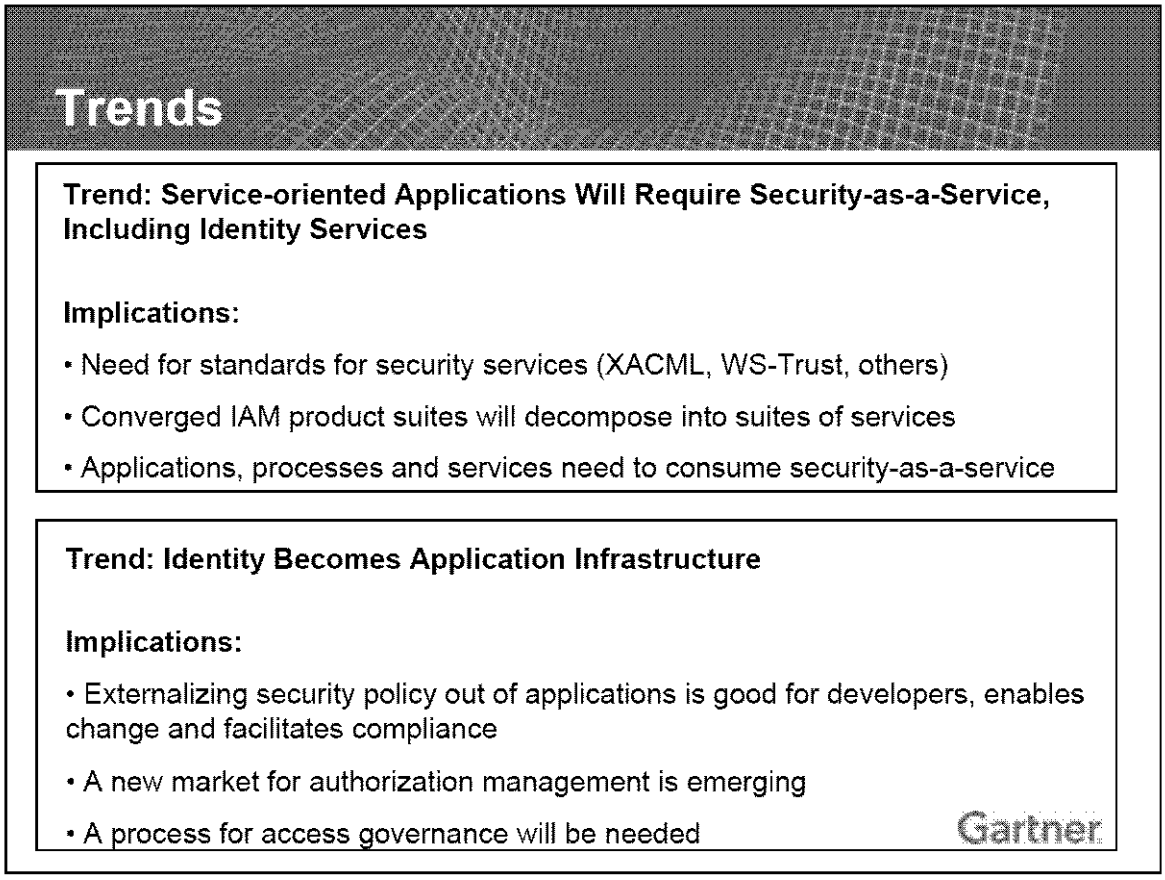
As SOA begins to drive application development, FTB will follow industry trends and will be able to shift accordingly. In the next 10 – 15 years, a shift from Web SSO to a wholly SOA should occur due to the following comparisons.

Figure 3.1-1: Comparison of Web SSO with IAM to SOA with AIM

Benefits and Drawbacks	
Web SSO with IAM	**SOA with IAM**
Relatively easy to deploy	Requires an in depth examination of processes, procedures and governance prior to deployment.
Mature technology – low deployment risk	Maturing technology – higher risk but higher reward
Provides a consolidated identity though account matching and system synchronization.	Provides a consolidated identity using either a centralized user repository or by creating a “virtual” database that joins disparate user databases.
System access is through a synchronization of accounts using “screen-scraping”	System access is verified by an identity provider in the form of a security assertion (token) containing user information that may include session, authentication and role data.
Typically used to grant access to “stove-piped” systems	Provides SSO capabilities for applications (service) that may also include composite applications. Stovepipe systems can be accessed with web-service “wrapping”

	technology.
Authentication is still controlled by individual applications	De-couples the authentication and authorization from applications and provides security to those systems as a service. This is a best practice
Most Web SSO solutions support Federated Identity	Supports Federated Identity
Does Not typically support user provision	Supports user provisioning
No Role Based Access Control	Most IAM solutions provide RBAC

Figure 3.1-2: Trends



Gartner – November 2007 IAM summit